

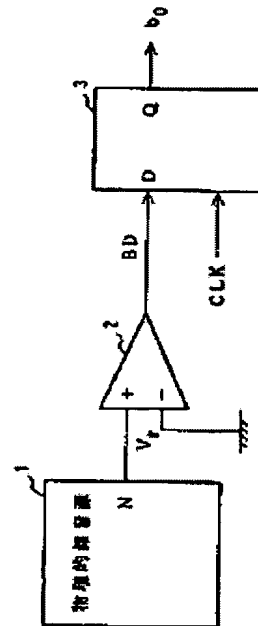
RANDOM NUMBER NOISE GENERATING SYSTEM

Patent number: JP2145010
Publication date: 1990-06-04
Inventor: YAMADA KUNIHIRO
Applicant: RICOH CO LTD
Classification:
- international: H03K3/84; H03B29/00
- european:
Application number: JP19880299360 19881125
Priority number(s):

Abstract of JP2145010

PURPOSE: To generate random number noise without reproducibility and periodically which is able to be converted into an optional distribution with high accuracy by binarizing noise outputted from a physical noise source at a prescribed threshold level, sampling the result at a prescribed frequency and outputting the result.

CONSTITUTION: The system is provided with a physical noise source 1, a comparator 2 as a binarizing means binarizing the noise outputted from the physical noise source 1, and a D flip-flop 3 receiving a binary output BD from the comparator 2 serially, sampling the signal synchronously with a clock CLK and outputting the result serially. When a reference voltage V_r of the comparator 2 is set to a ground potential, a noise outputted from a terminal N of the physical noise source 1 is sliced at a threshold level of a level '0' by the comparator 2, the result is outputted while being binarized into levels '1' and '0'. The reference voltage V_r of the comparator 2 is selected to be a prescribed value not being '0', then the probability of a binary output BD being '1' and the probability of being '0' are varied.



⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平2-145010

⑬ Int. Cl.⁹

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)6月4日

H 03 K 3/84
H 03 B 29/00

Z 8626-5J
8731-5J

審査請求 未請求 請求項の数 1 (全9頁)

⑮ 発明の名称 乱数雑音発生方式

⑯ 特 願 昭63-299360

⑰ 出 願 昭63(1988)11月25日

⑱ 発 明 者 山 田 邦 博 東京都大田区中馬込1丁目3番6号 株式会社リコー内

⑲ 出 願 人 株 式 会 社 リ コ ー 東京都大田区中馬込1丁目3番6号

明 細 書

1. 発明の名称

乱数雑音発生方式

2. 特許請求の範囲

物理的雑音源から出力される雑音を所定の閾値レベルで2値化し、該2値化出力を所定の周波数でサンプリングして出力するようになっていることを特徴とする乱数雑音発生方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、暗号システム用、シミュレーション用、あるいは実験測定用として利用される乱数、雑音を発生させる乱数雑音発生方式に関する。

〔従来の技術〕

従来、例えば1981年に発行された著者Donald E. Knuthによる文献「準数値算法 改訂第2版 Addison-Wesley社」に開示されているよう

に、計算機による乱数発生方式が以前から研究されている。計算機によって発生される乱数の特徴は、再現性があることであって乱数の性質を事前にかつ完全に調べることができるという利点があるが、例えば暗号システムにおける暗号鍵として乱数を用いる場合には、暗号鍵を有効に保護するために乱数には再現性がない方がよい。

このように暗号システム等の分野では再現性のない乱数、雑音を発生させることが望まれており、従来では、抵抗器等から発生する熱雑音、気体中の放電(例えばグロー放電)に伴う雑音、トランジスタやダイオードから発生するショット雑音等を適当に増幅して再現性のない乱数、雑音を発生させるようにしていた。例えばダイオードに高抵抗を通じて逆バイアス電圧を印加しダイオードをブレイクダウンさせることによって雑音を発生させるようにしていた。

〔発明が解決しようとする課題〕

抵抗器、トランジスタ、ダイオード等の上述した物理的雑音源からの熱雑音、ショット雑音、ブ

レークダウン雑音等によって、ある周波数帯域内では白色の乱数、雑音を発生させることができる。

しかしながら、これらの物理的雑音源は、温度、バイアス電圧等の影響を受け易く安定性に欠けるため一般には物理的雑音源からの雑音信号の直流分をコンデンサ等によって遮断し、雑音信号に周波数 f が“0”の付近の成分を含まないようにしていた。またトランジスタの $1/f$ 雑音、ポップコーン雑音等では周波数 f が“0”の付近で白色でないことが多い。このように物理的雑音源は不完全なものであったので、物理的雑音源を用いる場合には従来では周波数 f が“0”を含む広い帯域にわたって完全に白色の乱数、雑音を発生させることができないという問題があった。

さらに従来では得られた乱数、雑音は、正規分布をもつものに限られ、他の分布の乱数、雑音を得る場合には上記正規分布にさらに演算変換処理を施さなければならなかったため他の分布の乱数、雑音は精度が低くなるという問題があった。

さらには、上述した物理的雑音源で発生された

乱数、雑音をデジタル処理やコンピュータシミュレーション等を使用する場合には従来ではアナログ信号である雑音をA/D変換器でアナログ-デジタル変換していたので、A/D変換器の精度によって乱数、雑音の分解能が制約されてしまうという問題があった。すなわちコンピュータシミュレーション等においては 10^{-6} や 10^{-9} といった程度の分解能が乱数、雑音に要求され、このような分解能を得るためにはA/D変換器は1ワード当り20ビットや30ビットといった程度の精度を出すものでなければならないが、実際にはA/D変換器でこのような高精度を出すことはできないので、乱数、雑音の分解能を高くするには限界があった。

本発明は、不完全な物理的雑音源を用いた場合にも低周波数をも含む広い帯域で完全に白色のものであって、任意の分布に精度良く変換しうる再現性、周期性のない乱数、雑音を得ることが可能な乱数雑音発生方式を提供することを目的としている。

〔課題を解決するための手段〕

上記目的を達成するために、本発明は、物理的雑音源から出力される雑音を所定の閾値レベルで2値化し、該2値化出力を所定の周波数でサンプリングして出力するようになっていることを特徴としたものである。

〔作用〕

上記のような構成の乱数雑音発生方式では、物理的雑音源から出力される雑音を例えばコンパレータにより所定の閾値レベルで2値化し、この2値出力を例えばDフリップフロップにおいて所定の周波数でサンプリングして出力するようにしている。2値出力をサンプリングしてシリアルに出力する場合にサンプリングする周波数が高すぎなければ再現性、周期性のない乱数、雑音がDフリップフロップから得られる。また例えばDフリップフロップを縦続に接続したシフトレジスタによってコンパレータからの2値出力をサンプリングしてこれをパラレルに2値乱数系列として出力し、さらにシフトレジスタから順次出力される2値

乱数系列を相関のないように所定の周波数でサンプリングすることによって、周波数 f が“0”をも含む広い周波数帯域で白色の再現性、周期性のない一様分布の乱数、雑音を得ることができる。

〔実施例〕

以下、本発明の一実施例を図面に基づいて説明する。

第1図は本発明の第1の実施例のブロック図である。この実施例では、物理的雑音源1と、物理的雑音源1から出力される雑音を2値化する2値化手段としてのコンパレータ2と、コンパレータ2からの2値出力BDがシリアルに入力しこれをクロックCLKに同期させてサンプリングしてシリアルに出力するDフリップフロップ3とを備えている。

第2図は物理的雑音源1の一例を示す図であって、この物理的雑音源1では、ダイオード6に抵抗 R_1 、 R_2 を介して電源電圧Eを逆バイアスに加え、電源電圧Eをダイオード6のブレークダウン電圧よりも十分高くしてダイオード6にブレー

クダウンを生じさせ雑音を発生させるようにしている。

なお電源電圧Eに含まれる雑音を除去するためコンデンサC₁が設けられている。ダイオード6で発生した雑音は、抵抗R₃、R₄、R₅とコンデンサC₂、C₃とで定まる増幅率G(ω)で演算増幅器7によって増幅され端子Nから出力される。なおこの増幅率G(ω)は、演算増幅器6が理想的なものであるとすると、

$$G(\omega) = S\omega C_3 R_5 \cdot [1 + S\omega C_2 (R_3 + R_4)] / [(1 + S\omega C_2 R_4) \cdot (1 + S\omega C_3 R_5)] \quad \dots (1)$$

となる。

ここで、

$$C_2 (R_3 + R_4) = C_3 R_5 \quad \dots (2)$$

の関係が満たされれば、上記(1)式は、

$$G(\omega) = S\omega C_3 R_5 / (1 + S\omega C_2 R_4) \quad \dots (3)$$

となり、さらにR₃ >> R₄であれば、(2)式は

$$C_2 R_3 \doteq C_3 R_5 \quad \dots (4)$$

となるので、上記(3)式は、

$$G(\omega) \doteq (R_3 / R_4) \cdot [(S\omega C_2 R_4) / (1 + j\omega C_2 R_4)] \quad \dots (5)$$

となって、増幅率G(ω)はカットオフ周波数f_c(=1/(2πC₂R₄))を有し、カットオフ周波数f_c以下の低域を遮断する高域フィルタ特性を示す。

この特性によってダイオード6に加わる電源電圧Eがダイオード6から発生する雑音のレベルと比べて直流的に不安定であってもその影響を低減するようにしているが、反面、端子Nからはカットオフ周波数f_cよりも低域領域では良好な雑音成分が出力されず、周波数f_cよりも十分大きな周波数fの帯域においてほぼ白色の正規分布(ガウス分布)の雑音出力されるようになっている。なお白色となる周波数fの上限は演算増幅器7の特性によってほぼ決まる。

またコンパレータ2からの2値出力BDをサ

ンプリングするためのクロックCLKの周波数f_{CLK}は、自由に設定できてさらには周波数f_{CLK}は一定である必要さえないが、上述のように物理的雑音源1からの雑音は白色となる周波数fに上限があるので、この上限値以上にクロックCLKの周波数f_{CLK}を設定することはできない。また一般に高域フィルタのインパルス応答特性は、カットオフ周波数f_cの逆数1/f_cのオーダーの緩和時間をもつので、物理的雑音源1に白色正規分布とはみなせないような雑音成分(例えばポップコーン雑音)が含まれているような場合には、クロックCLKの周波数f_{CLK}が高いと1/f_cのオーダーの時間の間、互いに相関のある信号すなわち再現性、周期性をもつ乱数がDフリップフロップ3から出力される可能性がある。この影響をなくすためにはクロックCLKの周波数f_{CLK}をカットオフ周波数f_cよりも十分低く設定するのが良い。

このような第1の実施例では、物理的雑音源1から出力されるほぼ白色の正規分布をもった雑音

の平均、標準偏差、分散をそれぞれμ、σ、σ²とすると、μは雑音の平均直流電圧、σは雑音の平均直流電圧(実効値)、σ²は雑音の電力となる。

ここでコンデンサC₃によって直流分がカットされるので、平均直流電圧μは“0”である。

コンパレータ2の参照電圧V_rを第1図に示したように接地電位にすると、物理的雑音源1の端子Nから出力される雑音はコンパレータ2によって“0”の閾値レベルでスライスされて“1”と“0”とに2値化され出力される。雑音の平均直流電圧μが“0”であることから、2値出力BDが“1”となる確率、“0”となる確率はそれぞれ50%となる。

なお、コンパレータ2の参照電圧V_rを“0”でない所定の値とすることによって2値出力BDが“1”となる確率と“0”となる確率とを変化させることができる。例えば参照電圧V_rをσとすることによって2値出力BDが“1”となる確

率を約16%、"0"となる確率を約84%にすることができる。但し、第2図の物理的雑音源1は演算増幅器6の高域フィルタ特性を使用しており、この物理的雑音源1では高域のカットオフ周波数が不安定であるので、フィルタの帯域幅が変化しフィルタの帯域幅に比例する分散 σ^2 も不安定となる。従って参照電圧 V_r を σ にする場合には、 σ を安定させるため安定したCR定数によって規定される通常のバンドパスフィルタを採用するのが良い。第1図に示したように、参照電圧 V_r を"0"にする場合には、分散の σ^2 の大きさによって2値出力BDが"1"となる確率、"0"となる確率がそれぞれ50%から変化することはないので、バンドパスフィルタを設けて高域をカットせずとも良い。

このようにして参照電圧 V_r を例えば"0"にしたときにコンパレータ2によって"1"、"0"に2値化された2値出力BDは、Dフリップフロップ3にシリアルに投入し、クロックCLKによってサンプリングされる。この結果、Dフリップ

フロップ3からはクロックCLKのタイミングに合わせてランダムな2値系列がシリアルなデータ b_0 として出力される。

なお擬ランダムな2値系列としては、例えば1971年に発行された著者G. Hoffmann de Vismeによる文献「2値系列(Binary Sequences) The English Universities Press Ltd.」に開示されているようなM系列が有名である。

M系列は線形フィードバックシフトレジスタによって簡単な構成で発生できるという利点があるが、再現性および周期性があるという欠点をもっている。

これに対して、上述したような第1の実施例では、クロックCLKの周波数 f_{CLK} をカットオフ周波数 f_c よりも十分低く設定することなどによって、Dフリップフロップ3からのシリアルなデータ b_0 を安定性を有しかつ再現性、周期性がないランダムな2値系列として出力させることができる。

第3図は本発明の第2の実施例のブロック図で

ある。この実施例では、物理的雑音源1と、物理的雑音源1から出力される雑音を2値化する2値化手段としてのコンパレータ2と、コンパレータ2からの2値出力BDがシリアルに投入し、クロックCLKに同期させてサンプリングしてパラレルに出力するシフトレジスタ8と、"n-1"まで順次に計数し"n-1"の次に再び"0"に戻るモジュロnカウンタ(modulo-nカウンタ)9と、モジュロnカウンタ9が例えば"0"となるたびにシフトレジスタ8からのパラレル出力をラッチするラッチ回路10とを備えている。

第4図はシフトレジスタ8の具体的な構成を示す図である。シフトレジスタ8は、n個のDフリップフロップ3-1乃至3-nを縦続接続して構成されており、第1図に示したような1つのDフリップフロップ3からのシリアルデータ出力を後続のDフリップフロップに順次に伝送しパラレルデータに変換して出力するようになっている。

このような第2の実施例では、参照電圧 V_r を例えば"0"にしたときにコンパレータ2によっ

て"1"、"0"に2値化された2値出力BDはシフトレジスタ8にシリアルに投入し、クロックCLKによってサンプリングされてシフトレジスタ8のDフリップフロップ3-1乃至3-nに順次に転送され、各Dフリップフロップ3-1乃至3-nからn個の2値乱数系列 b_0 乃至 b_{n-1} としてパラレルに出力される。これらのn個の2値乱数系列 b_0 乃至 b_{n-1} をnビットのバイナリワードとみなすときに、これは一様分布の乱数となる。このようにしてシフトレジスタ8から出力されるn個の2値乱数系列 b_0 乃至 b_{n-1} はクロックCLKが入力されるたびにすなわち系列が1つずれるごとにラッチ回路10に送られる。

ところで、モジュロnカウンタ4はクロックCLKがn個出力されるごとに1つのストローブ信号STB₁をラッチ回路10に送り、これによってラッチ回路10ではシフトレジスタ8からのn個の2値乱数系列 b_0 乃至 b_{n-1} をストローブ信号STB₁が送られたときにのみすなわちクロックCLKがn回生起したときにのみラッチする。

これによってラッチ回路10でストローブ信号 STB_1 ごとに順次にラッチされる n 個の2値乱数系列 b_0 乃至 b_{n-1} すなわち n ビットのバイナリワード間の相関をなくすることができて、ラッチ回路10から再現性、周期性のない一様分布の乱数を発生させることができる。

またストローブ信号 STB_1 の周波数すなわちラッチ回路10における2値乱数系列 b_0 乃至 b_{n-1} のサンプリング周波数を f_p とすると、離散時間系での意味において周波数“0”から“ $f_p/2$ ”までの全周波数帯域においてラッチ回路10から出力される n ビットのバイナリワード b_0 乃至 b_{n-1} を白色のものとする事ができる。

このようにして、第2の実施例では、物理的雑音源1が不完全なものであっても、物理的雑音源1からの雑音を2値化し適正な周波数 f_{CLK} 、 f_p のクロック CLK 、ストローブ信号 STB_1 でサンプリング処理することによって、低周波数をも含む広い帯域で完全に白色であってかつ再現性、周期性のない一様分布の乱数、雑音を得るこ

とが可能となる。

第5図は上述した第2の実施例で得られた一様分布の乱数、雑音を正規分布、ポアソン分布等の任意の分布に変換する変換手段の一例を示す図である。第5図では変換手段として読出し専用メモリ(ROM)11が用いられており、ROM11に所定の分布への変換用関数をテーブルとして記憶させ、ラッチ回路10からの n ビットの2値乱数系列 b_0 乃至 b_{n-1} をROM11へのアドレスとして入力させている。

例えば変換用関数として、誤差関数 $\text{erf}(g)$ ($= (2\pi)^{-1/2} \int_0^g e^{-x^2/2} dx$) の逆関数 $\text{erf}^{-1}(g)$ を用いれば、一様分布を正規分布(ガウス分布)に変換することができて、ROM11からは、広い周波数帯域にわたって白色の正規分布の乱数、雑音を変換データとして出力させることが可能となる。

なお、ROM11へのアドレス入力は n ビットの2値乱数系列であるので 2^n の分解能を有し、

ROM11において一様分布を正規分布に変換する場合に、 2^{-n} や $1-2^{-n}$ の確率に相当するアドレス入力によって変換データの最小値、最大値が決まってしまう。例えば n が“16”であれば、 $-4 \cdot 2\sigma_1 \sim 4 \cdot 2\sigma_1$ 程度までしか変換することができず、その意味では変換データは不完全な正規分布であり、極めて高い精度のものとはなっていない。なお σ_1 はROM11において変換された正規分布の標準偏差である。

第6図はアドレス入力のビット数 n が有限であることによって生ずる変換された正規分布の不完全さを統計学における中心極限定理を利用して取除き修正するための一例を示す構成図である。

第6図ではROM11からの変換データの不完全な正規分布を修正する手段として、アキュムレータ12と、ROM11からの出力とアキュムレータ12の内容とを加算し加算結果をアキュムレータ12に蓄積させる加算器13と、モジュロ n カウンタ9からのストローブ信号 STB_1 を“ $m-1$ ”まで順次に計数し“ $m-1$ ”の次に再

び“0”に戻るモジュロ m カウンタ14と、モジュロ m カウンタ14が例えば“0”となるたびにモジュロ m カウンタ14から出力されるストローブ信号 STB_2 を遅延する遅延回路15と、ストローブ信号 STB_2 によってアキュムレータ12に蓄積された加算結果をラッチし出力するレジスタ16とを備えており、上記アキュムレータ12は、遅延回路15からの遅延されたストローブ信号 STB_2 によってクリアされ、またアキュムレータ12は、モジュロ n カウンタ9からのストローブ信号 STB_1 に同期して加算器13から加算結果を取込み加算結果を更新するようになっている。

このような構成では、ROM11からストローブ信号 STB_1 のタイミングごとに一個一個出力される変換データを m 回順次に加算し、その加算結果をレジスタ16から出力するようにしている。中心極限定理は、一個一個が不完全な正規分布のものであっても互いに独立な多数の正規分布が合わさることによってより完全な正規分布に近づけ

ることができるという原理であって、ROM 11からストローブ信号STB₁ごとに出力される確率変数としての上述した変換データは互いに相関がなく独立なものである。この中心極限定理が適用され、これによって、レジスタ16から出力される加算結果をより完全な正規分布の変換データとして得ることができる。例えばn、mをそれぞれ“16”とし、ROM 11から出力される変換データの分散を σ_1^2 とすると、レジスタ16から出力される変換データの分散は $16\sigma_1^2$ となる。一方、ROM 11から出力される変換データは、最小値 $-4 \cdot 2\sigma_1$ と最大値 $4 \cdot 2\sigma_1$ との間の値をとるので、レジスタ16から出力される変換データは最小値 $(-4 \cdot 2\sigma_1 \times 16)$ と最大値 $(4 \cdot 2\sigma_1 \times 16)$ との間の値をとることになる。レジスタ16からの変換データの分散を σ_1^2 に規格化すると、レジスタ16からの変換データは最小値 $(-4 \cdot 2\sigma_1 \times 16 / \sqrt{16})$ と最大値 $(4 \cdot 2\sigma_1 \times 16 /$

$\sqrt{16})$ との間の値、すなわち $-16 \cdot 8\sigma_1 \sim 16 \cdot 8\sigma_1$ の範囲をもつことになり、極めて精度の高いものにすることができる。この例では、加算結果を得るのに時間的に直列に加算したが、物理的雑音源1、コンパレータ2、シフトレジスタ8、ラッチ回路10、ROM 11をそれぞれ複数個用意して並列加算するようにしても良い。

このようにして不完全な物理的雑音源1を用いた場合にも、極めて精度の高い白色の正規分布の乱数、雑音を得ることができる。

なお、通常はコンパレータ2の閾値レベルのオフセットは十分小さなものであるが、極めて精度の高い乱数、雑音を得ようとする場合にはコンパレータ2のオフセットが問題となる。例えば参照電圧 V_r が“0”よりも等価的に低くオフセットしたような場合には、コンパレータ2からの2値出力は“1”の出力される確率が“0”の出力される確率よりも偏かに大きくなり、結果的にレジスタ16から出力される変換データの平均値 μ_1 が正確には“0”ではなくなり精度を低下させる。

このような問題を回避し、レジスタ16から出力される変換データの平均値 μ_1 を正確に“0”となるようにするためには第6図に示すアキュムレータ12、加算器13の構成を第7図に示すように変更すれば良い。すなわちROM 11からの変換データをm回加算する第6図の加算器13のかわりに、第7図では $m/2$ 回加算し、 $m/2$ 回減算する加減算器17を設けている。この加減算器17とアキュムレータ12との組合わせによって、ROM 11からストローブ信号STB₁ごとに出力される変換データ G_1, G_2, \dots, G_n を、
 例えは $\sum_{i=1}^{n/2} (G_{2i} - G_{2i-1})$ のように加減算して

アキュムレータ12からレジスタ16に出力させる。加算を減算に置き換えても、変換データの分散 $m \times \sigma_1^2$ には影響を与えず、分散は第6図に示す加算だけの場合と同じに保たれる。これに対して平均値 μ_1 は加算と減算とによって打消され、上述の例においてmが偶数である場合には加算、

減算は同一回数なされるので平均値 μ_1 は完全に打消されこれを“0”にすることができる。

このようにして、第7図の構成ではコンパレータ2の閾値レベルにオフセットがある場合にも、この影響を除いて極めて精度の高い乱数、雑音を得ることが可能となる。

以上のようにして得られた乱数、雑音をシミュレーション用、実験測定用に使用すれば、これによって極めて精度の高いシミュレーション、測定が可能となる。また暗号鍵の生成に使用すれば、どのような鍵が生成されたか第三者には全く予想がつかずこれを有効に保護することができる。

(発明の効果)

以上に説明したように、本発明によれば、物理的雑音源から出力される雑音を所定の閾値レベルで2値化し該2値出力を所定の周波数でサンプリングして出力するようにしているので、物理的雑音源が不完全なものであっても低周波数をも含む広い帯域で完全に白色のものであって、任意の分布に精度良く変換しうる再現性、周期性のない乱

数、雑音を得ることができる。

4. 図面の簡単な説明

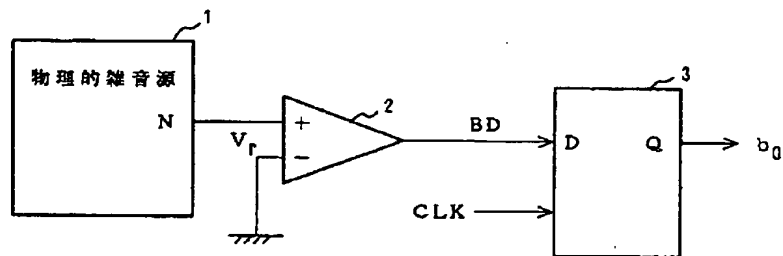
第1図は本発明の第1の実施例のブロック図、第2図は第1図に示した物理的雑音源の一例を示す図、第3図は本発明の第2の実施例のブロック図、第4図は第3図に示したシフトレジスタの具体的な構成図、第5図は一般分布の乱数、雑音を任意の分布に変換する変換手段を第3図の構成に追加した場合の一例を示す図、第6図は一般分布の乱数、雑音を正規分布に変換したときに正規分布の不完全さを中心極限定理を利用してより完全な正規分布に修正する修正手段を第5図の構成に追加した場合の一例を示す図、第7図は第6図に示した修正手段の他の例を示す図である。

- 1…物理的雑音源、2…コンパレータ、
- 3, 3-1乃至3-n…Dフリップフロップ、
- 6…ダイオード、7…演算増幅器、
- 8…シフトレジスタ、9…モジュロnカウンタ、
- 10…ラッチ回路、11…ROM、

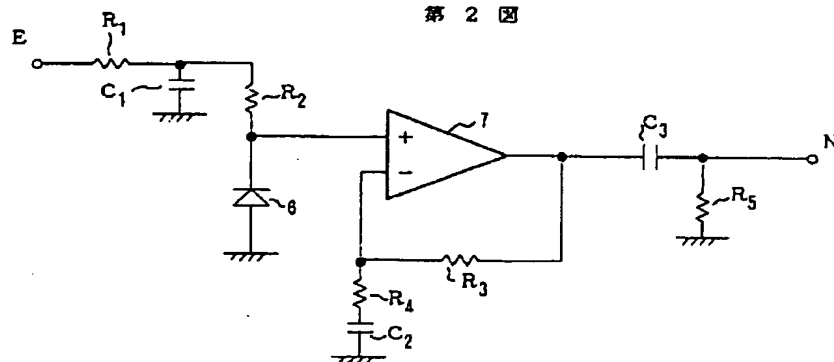
- 12…アキュムレータ、13…加算器、
- 14…モジュロmカウンタ、15…遅延回路、
- 16…レジスタ、17…加減算器、
- V_r …参照電圧、BD…2値出力、
- b_0 乃至 b_{n-1} …2値乱数系列、
- CLK…クロック、
- STB₁, STB₂…ストローブ信号、
- f_{CLK} …クロックCLKの周波数、
- f_p …ストローブ信号STB₁の周波数

特許出願人 株式会社 リ コ ー

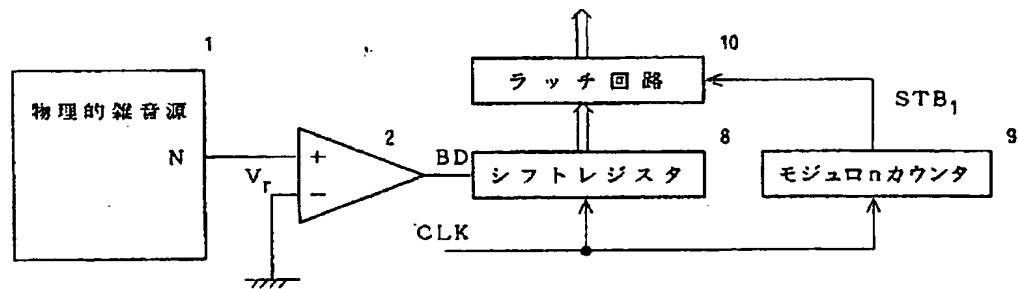
第1図



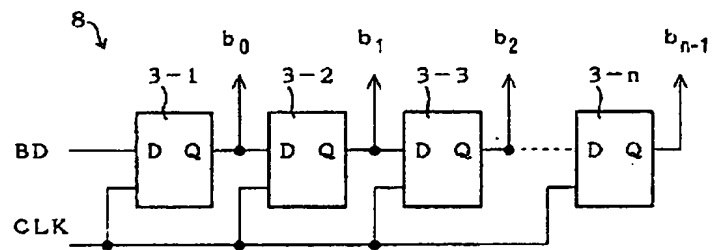
第2図



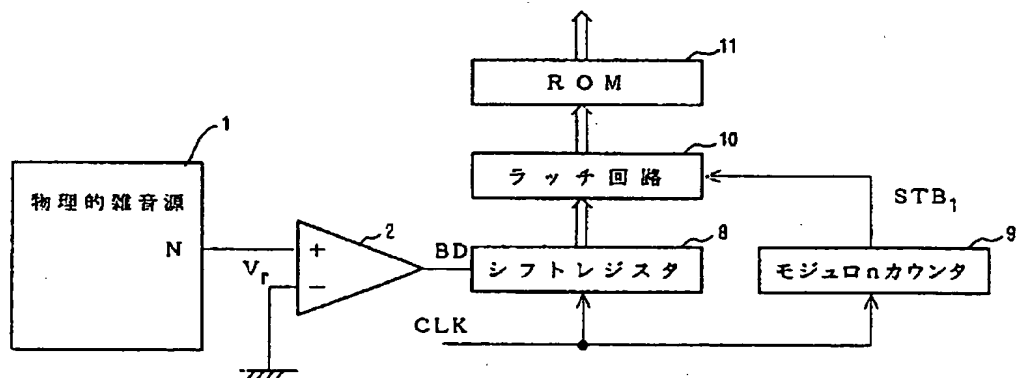
第 3 図



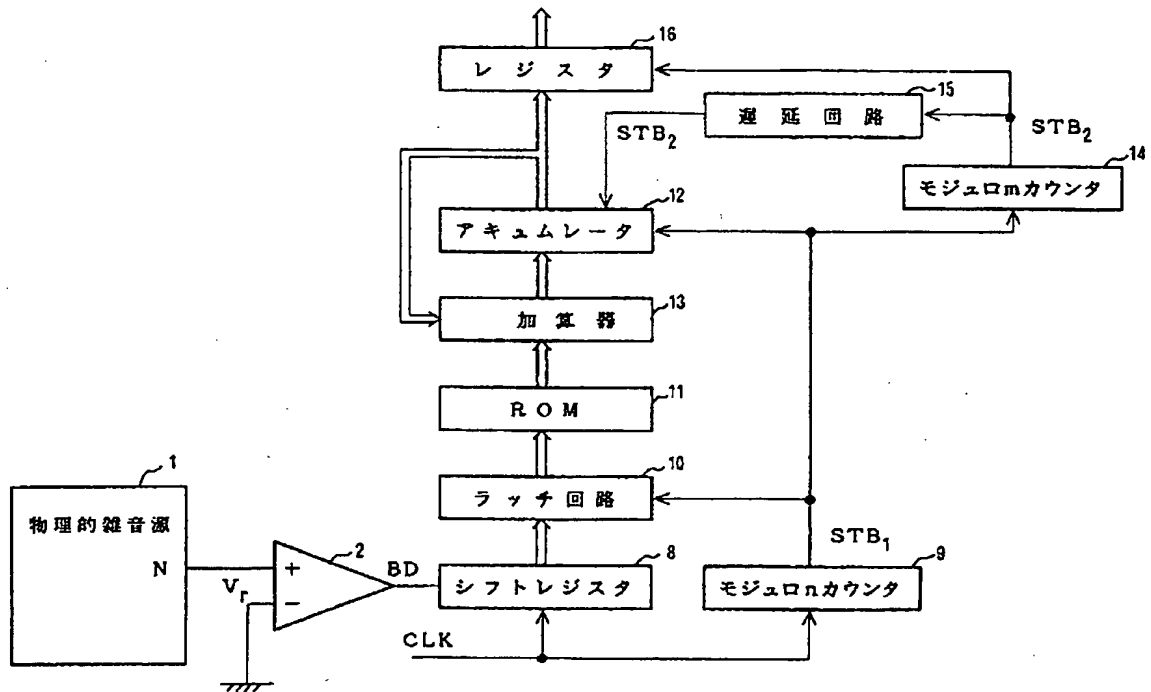
第 4 図



第 5 図



第 6 図



第 7 図

